

Incident Response Tools

James Madison University Dept. of Computer Science

June 13, 2015

1 Introduction

Being successfully attacked is inevitable. A determined hacker WILL be able to penetrate your network.

The attacker, if they want to re-enter your network, will have to leave a backdoor somewhere. This means they will likely re-add guest accounts, disable firewall ports, and re-enable services that you had previously disabled (in the Windows Security Exercise...like FTP) to provide a means for them to access your computer easily.

In this chapter, we will briefly re-examine things talked about in the Windows Security Exercise that are relevant after an incident and then we will cover new tools that will help you investigate an incident.

All tools necessary are available on the Desktop of your IR Tools snapshot.

2 Services

Knowing what services are running on your windows machine is very important, especially after being attacked. Having extra services running that are not necessary may add vulnerabilities to your machine and may allow an attacker to re-enter your network. The more services that are running on a machine means the more services you must protect and secure. By default, many software packages install many extra side services you do not want to be running, and as good network administrator you must be aware of these.

2.1 What Services are running?

All Microsoft Windows Server Editions have a Graphical User Interfaces to help manage the machine's services. The GUI to manage what services are running can be accessed in the Start Menu under Administrative Tools by clicking on Services. Figure 1 shows how to access the services GUI from the start menu.

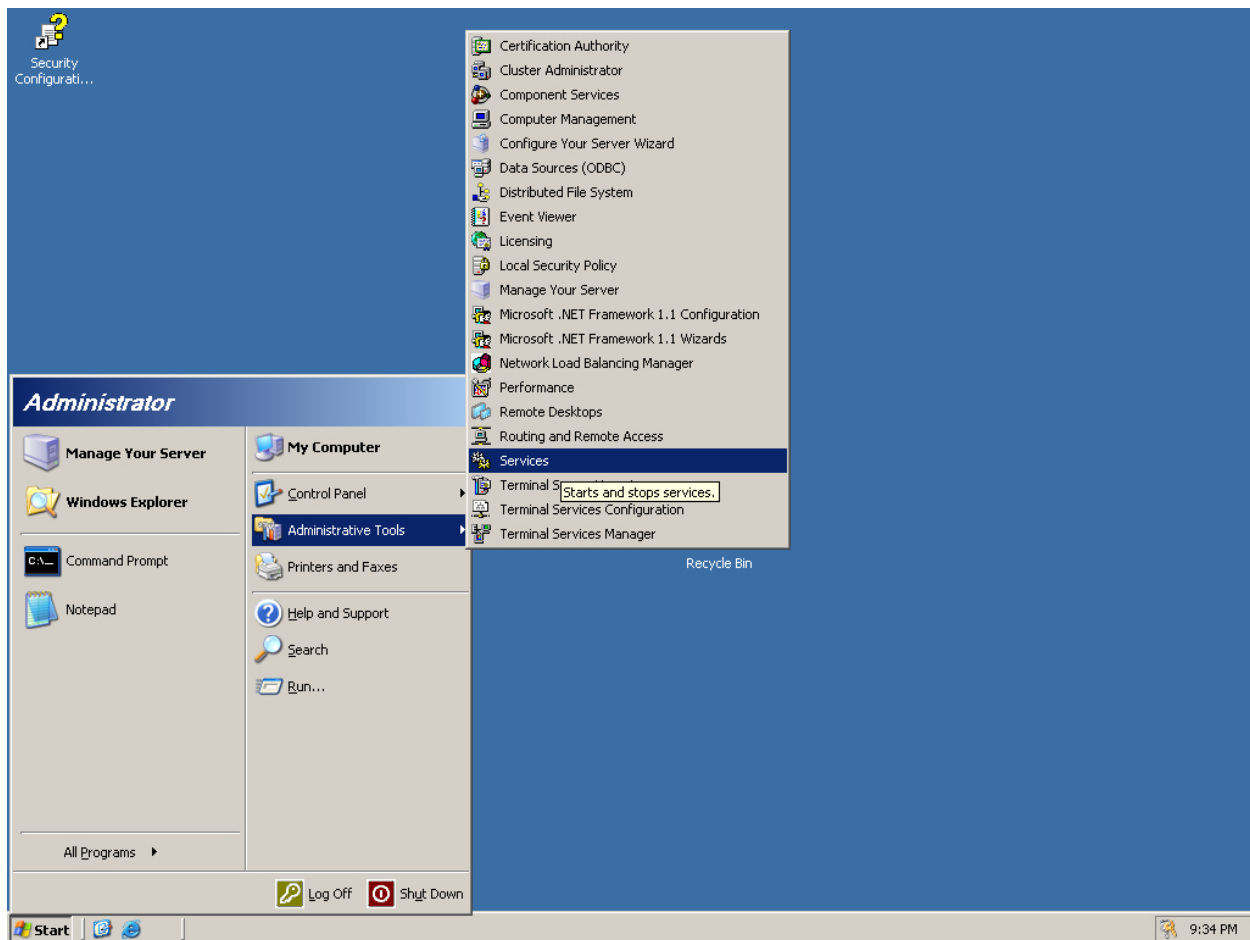


Figure 1: Click on Services to manage what services are running

By default, the list of things on this list is large and difficult to sort through but we will only be looking at a few choice things. By default, Windows Firewall is Disabled. This is a very important service. An attacker, wanting to regain access to your system later, may have disabled Windows Firewall. To turn it back on double click on it, change "Disabled" to "Automatic", and then Press "Start". Figure 2 shows how to do this.

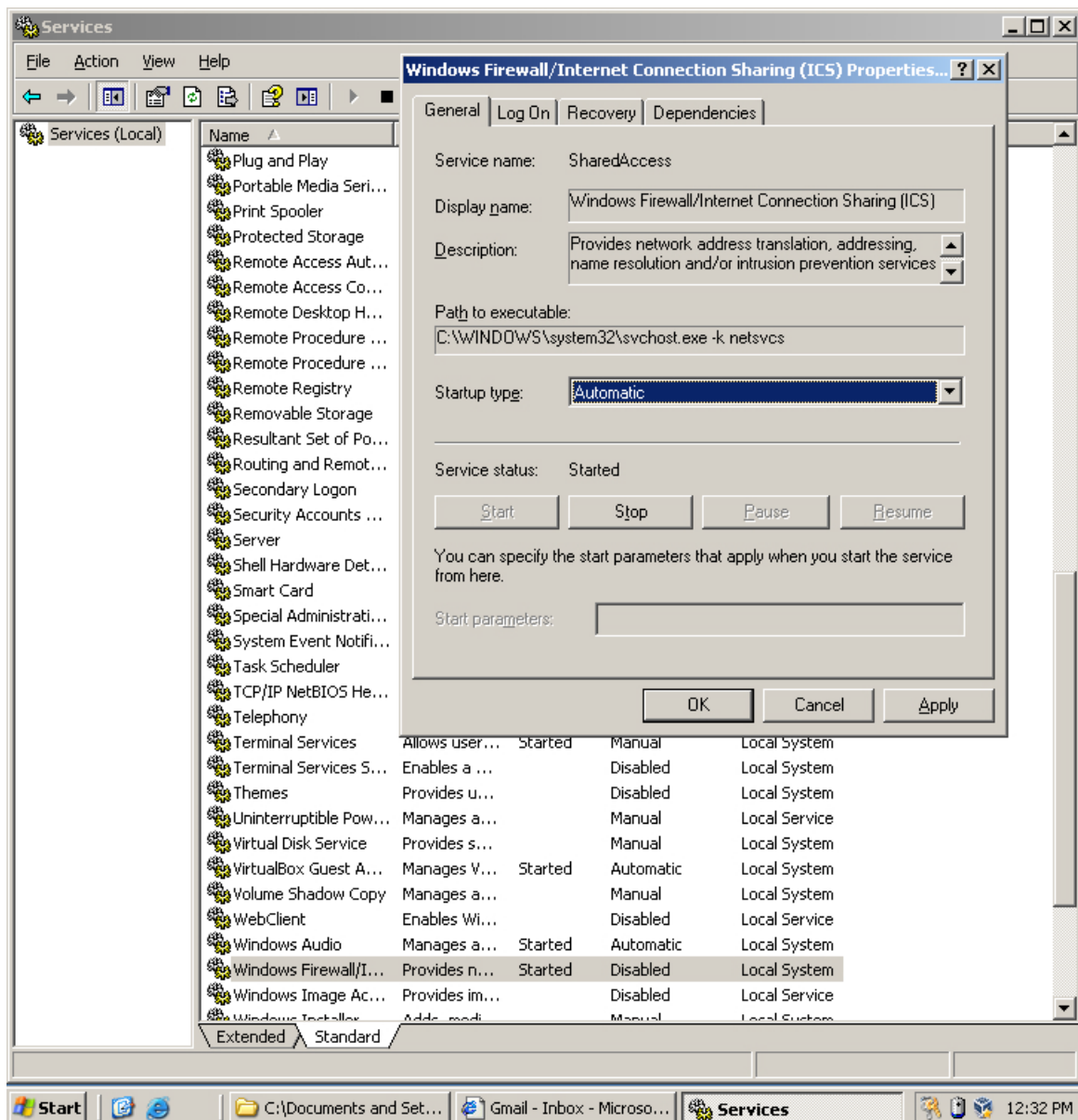


Figure 2: Change Setup type to Automatic to turn the firewall on.

You may also notice that the File Transfer Protocol may be enabled. It is very important that this protocol, and Telnet, are disabled and they should always stay disabled. These protocols are used so remote users can authenticate and use your computer. Remote Authentication is a standard practice, but FTP and Telnet do not do it securely. If you see SSH or Very Secure File Transfer Protocol these services are okay to use. After an attacker enters your system they may re-enable FTP or Telnet in order to access your machine later. They may think that the

system administrator may not notice since they were likely disabled to begin with. This is why it is so important to check and re-disable these services if they have been enabled.

3 Firewalls

All Windows distributions come with a built in host based firewall that you can configure. In the real world many companies buy expensive machines that serve solely as a firewall. Even though the Windows Firewall is not expensive and dedicated hardware it is a great line of defense to keep attackers from accessing ports on your computer that may have a vulnerability. It will also protect your computer from attacks that originate from inside your network. It is very easy to understand how a firewall works. People connect to your computer through ports and a firewall blocks ports. An easy way to think about ports is a lot of tiny mailboxes. Anytime someone wants to communicate with your server they put mail in a particular mailbox. Each port is for a different purpose. A firewall will block these mailboxes so nobody can put anything in them. This decreases the surface area a hacker could attack you with.

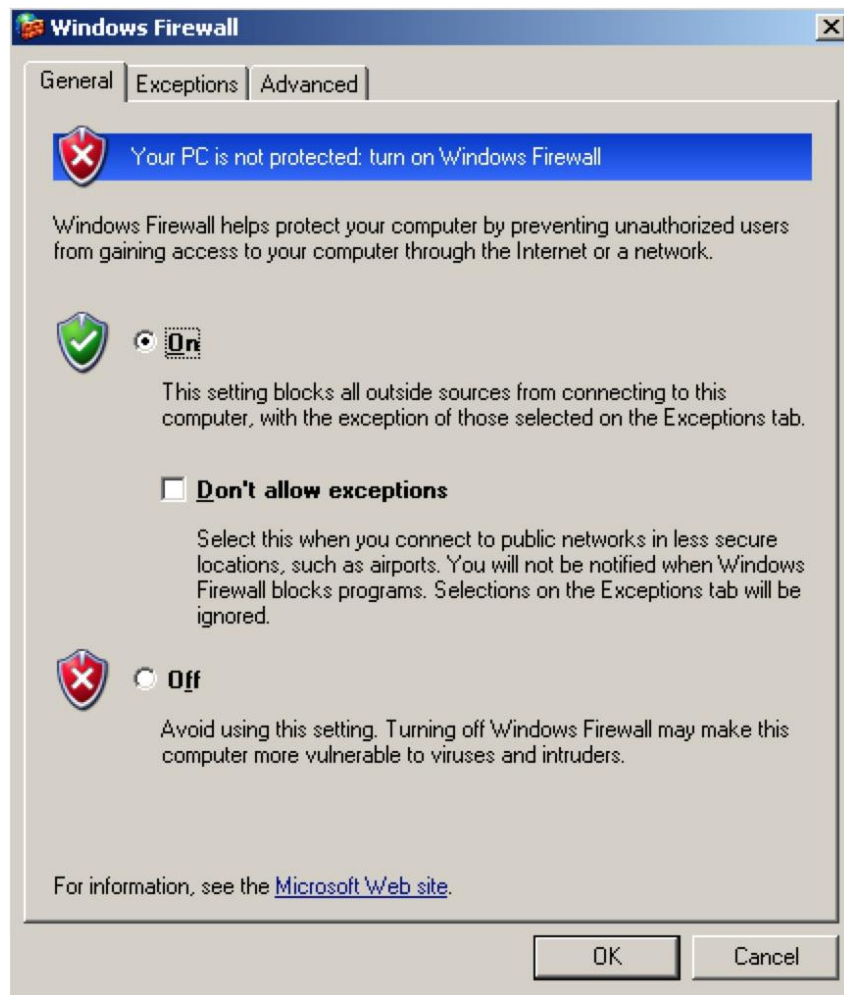


Figure 3: Change Setup type to Automatic to turn the firewall on.

To use the Windows Firewall you must first enable it. Windows Firewall can be found in the Control Panel. After clicking on Windows Firewall you should see a user interface like the one in Figure 3. Change Windows Firewall from off to on and then click the Advanced tab at the top of the interface.

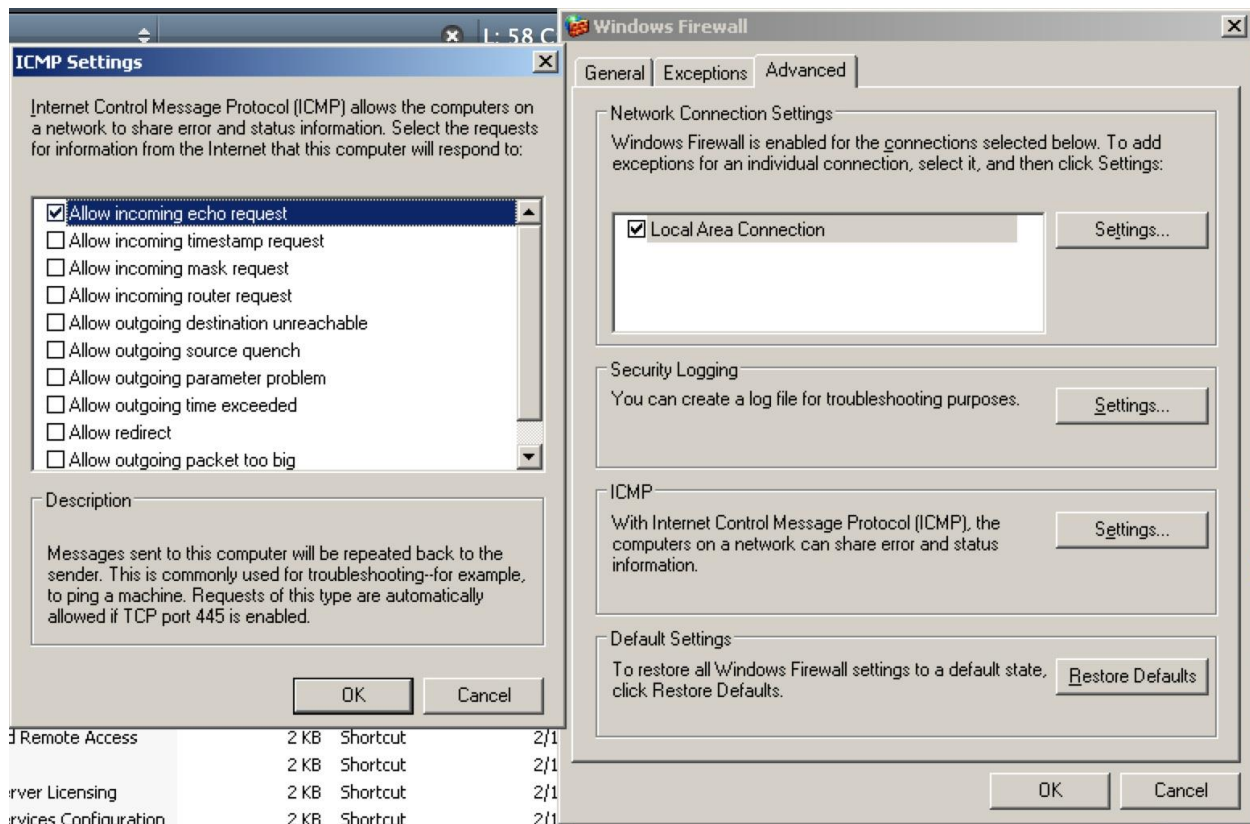


Figure 4: Click Settings and check Allow incoming echo request.

In the advanced tab, click Settings within the ICMP settings. When the ICMP Settings user interface pops up select Allow incoming echo requests and then Ok. This allows other computers to ping your computer. Ping is special and does not use a port, but your firewall is still able to block it. Next click on the Exceptions tab at the top of the Windows Firewall. These instructions are reflected in Figure 4

Click on the Add Port button in the Exceptions tab to add exceptions to the Firewall. By default Windows Firewall will block all ports and you will only open the ones you need. This is much easier than leaving all open and blocking the ones you don't want because there are more than sixty-five thousand ports. Your computer will be running a Webserver and web servers generally use port 80 to communicate with computers that request webpages. Figure 5 shows you how to unblock port 80. After pressing Ok in Windows Firewall, your Firewall changes will take affect and your firewall will be active. You should also do the same with port

23 which is Telnet (we will go into why later, yes Telnet is insecure and in general should not be used, but we have a very specific reason).

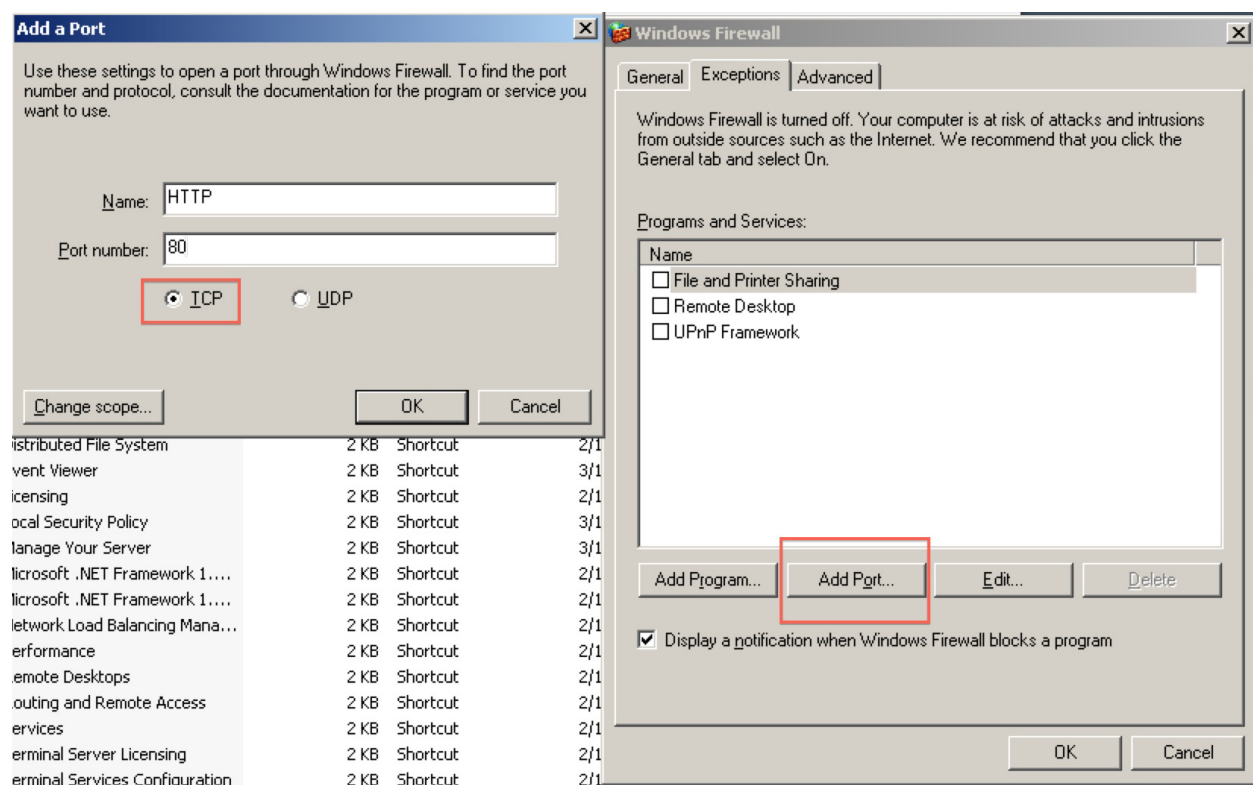


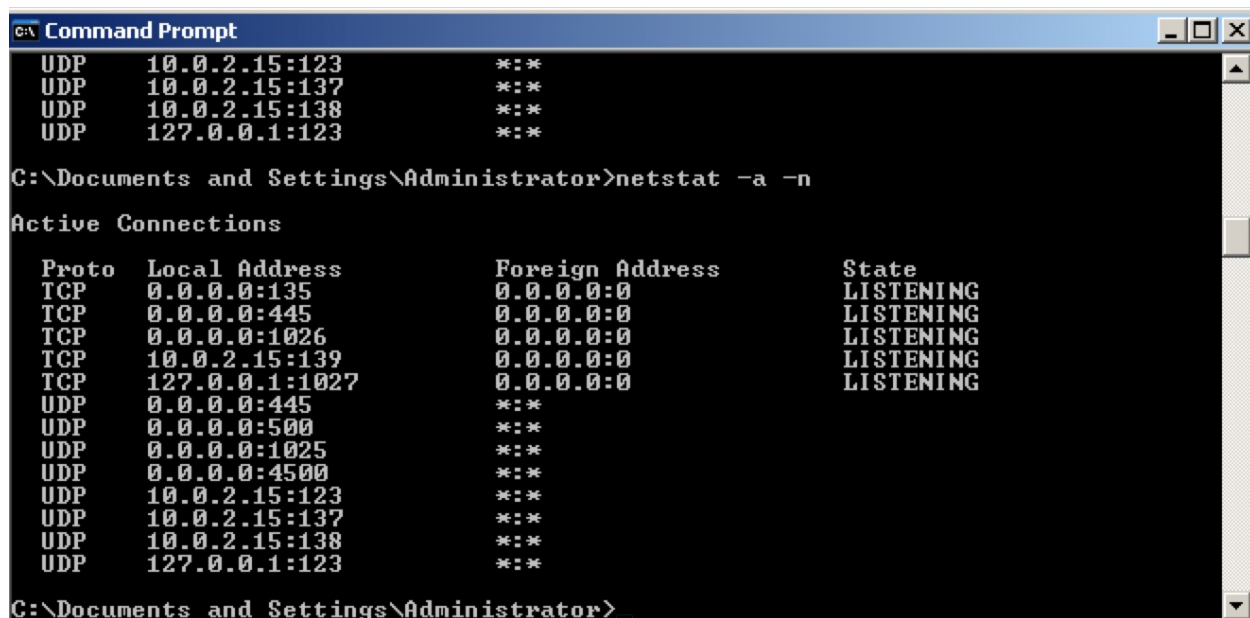
Figure 5: Make sure to select TCP after hitting pressing Add Port.

4 Command Line Tools

The command line is a powerful tool that can help a defender get important information quickly and easily. There is a little bit of a learning curve when using the command line, and almost nobody knows every command there is, but learning how to use a few basic commands is quick and easy. To open the command line, click to open the Start menu and click Command Prompt, or press Windows Key + R and type cmd.exe. In these tutorials we will only scratch the surface of the things these commands can do. If you want to learn more about a particular command, you can do so by typing command help into the terminal, where "command" is the command you want more information on.

4.1 netstat

Netstat is a powerful command line tool that lists important networking information about your computer. The main uses for netstat is to show open network connections. To read comprehensive documentation about netstat you can read <https://technet.microsoft.com/en-us/library/bb490947.aspx>. Netstat will show who and what is currently connected to your computer. This is an extremely important thing to know. If an attacker was to hack your computer, they would have to communicate with your computer over the network in order to interact with it. Using netstat you could see if a hacker is currently connected to your computer and take steps to kick him out. In the command line window type netstat -an. The -an is used to specify exactly what information you want to show. -a means netstat will show all active connections. -n means netstat will show all ports your computer is listening for active connections on. After typing netstat -an and hitting enter your terminal should look similar to the command line window in Figure 6.



```
C:\ Command Prompt
UDP    10.0.2.15:123      *:*
UDP    10.0.2.15:137      *:*
UDP    10.0.2.15:138      *:*
UDP    127.0.0.1:123      *:*

C:\Documents and Settings\Administrator>netstat -a -n

Active Connections

Proto Local Address          Foreign Address         State
TCP   0.0.0.0:135            0.0.0.0:0               LISTENING
TCP   0.0.0.0:445            0.0.0.0:0               LISTENING
TCP   0.0.0.0:1026           0.0.0.0:0               LISTENING
TCP   10.0.2.15:139          0.0.0.0:0               LISTENING
TCP   127.0.0.1:1027         0.0.0.0:0               LISTENING
UDP   0.0.0.0:445            *:*
UDP   0.0.0.0:500           *:*
UDP   0.0.0.0:1025           *:*
UDP   0.0.0.0:4500          *:*
UDP   10.0.2.15:123          *:*
UDP   10.0.2.15:137          *:*
UDP   10.0.2.15:138          *:*
UDP   127.0.0.1:123          *:*

C:\Documents and Settings\Administrator>
```

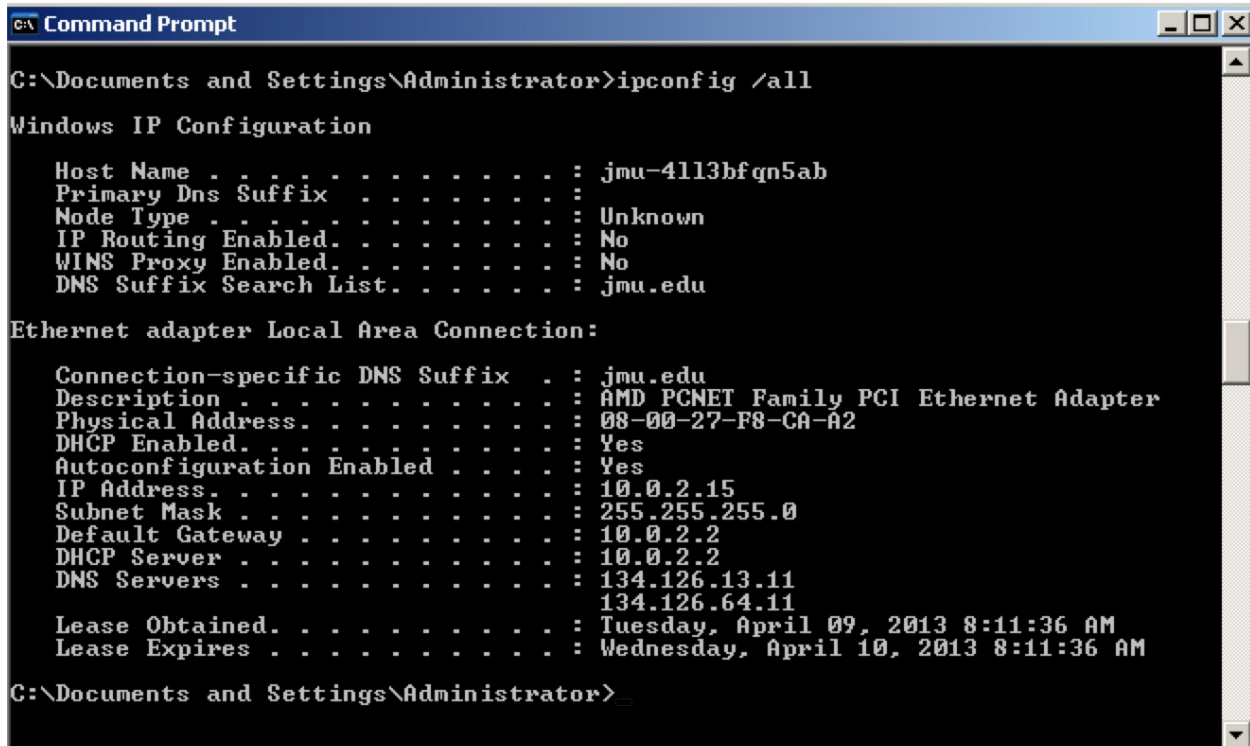
Figure 6: Output from a netstat -an command

This shows you what it looks like when there are no active connections but what will it look like when you do have an active connection? In order to test this and see how netstat changes, open a web browser and enter google.com into the URL bar and hit enter. Re-enter netstat -an into the terminal and view how the output

changes. There are now connections connecting to a foreign address that you can see. This is because your computer establishes a connection with Google in order to communicate and ask Google to send you their webpage. Open a new webpage and see how netstat changes. It may sometimes be difficult to identify good versus bad connections on your computer. Generally a connection to a port that you should not need is bad. An example of this would be a webserver that only needs to allow connections to port 80. Connections you see to port 80 are more than likely good, but if netstat shows a connection on port 21, 22, or 23 to a remote address then it is highly likely that your computer has been compromised. Also check for your computer connecting to foreign address on high number ports.

4.2 ipconfig

ipconfig is a command line program that can be used to show the networking information of your computer. It will show things like your IP address, physical address, and DNS server.



```
C:\> Command Prompt
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : jmu-4113bfqn5ab
Primary Dns Suffix . . . . . : 
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : jmu.edu

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : jmu.edu
Description . . . . . : AMD PCNET Family PCI Ethernet Adapter
Physical Address. . . . . : 08-00-27-F8-CA-A2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2
DHCP Server . . . . . : 10.0.2.2
DNS Servers . . . . . : 134.126.13.11
                        134.126.64.11
Lease Obtained. . . . . : Tuesday, April 09, 2013 8:11:36 AM
Lease Expires . . . . . : Wednesday, April 10, 2013 8:11:36 AM

C:\Documents and Settings\Administrator>
```

Figure 7: Output from ipconfig /all command

This tool is not a great tool to keep hackers out of your computer. It is more a tool to use when you first sit down on your computer. It may be useful to note your IP address, DNS Server, gateway, and physical address. These values are not static and you may notice them change, but if you notice these things changing often it may be a sign an attacker has played with your networking configuration.

5 SysInternals

Sysinternals is a suite of free tools that help users better understand what is happening on the computer. They are all available, along with tutorials and documentation, at <http://technet.microsoft.com/enus/sysinternals/>. In this document we will demonstrate a few of the best tools in the suite. If you wish to download all Sysinternals tools, you can at <http://download.sysinternals.com/files/SysinternalsSuite.zip>, but all tools are already installed to your desktop in the Sysinternals folder. What is covered in this tutorial is by no means comprehensive. The Sysinternals suite has so many uses and even the tools we cover have many uses beyond the scope of this tutorial. If you have extra time try loading up a tool that sounds interesting and see what you can figure out.

5.1 TCPView

TCPView is a program written by Microsoft that helps you see networking information for your computer. It is very similar to netstat but in a graphical form. It can be downloaded from <http://download.sysinternals.com/files/TCPView.zip>. To run it double click on 'tcpview.exe' in the Sysinternals folder. The graphical user interface will show current, active TCP connections. If an attacker is communicating with your computer you may see a suspicious connection. An example of this would be something like Notepad.exe using a TCP port to communicate with a remote host. Notepad should never be communicating over the network.

The screenshot shows the TCPView application window with the following data:

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets
IEEXPLORE.EXE	1728	UDP	imujmu-ae53p0f4	1027	*	*		
lsass.exe	540	TCP	imujmu-ae53p0f4	1025	imujmu-ae53p0f4	0	LISTENING	
lsass.exe	540	UDP	imujmu-ae53p0f4	isakmp	*	*		
lsass.exe	540	UDP	imujmu-ae53p0f4	ipseccm	*	*		
svchost.exe	860	TCP	imujmu-ae53p0f4	epmap	imujmu-ae53p0f4	0	LISTENING	
svchost.exe	916	UDP	imujmu-ae53p0f4	1036	*	*		
svchost.exe	916	UDP	imujmu-ae53p0f4	1028	*	*		
svchost.exe	944	UDP	imujmu-ae53p0f4	ntp	*	*		
svchost.exe	944	UDP	imujmu-ae53p0f4	ntp	*	*		
System	4	TCP	imujmu-ae53p0f4	microsoft-ds	imujmu-ae53p0f4	0	LISTENING	
System	4	TCP	imujmu-ae53p0f4	netbios-ssn	imujmu-ae53p0f4	0	LISTENING	
System	4	UDP	imujmu-ae53p0f4	microsoft-ds	*	*		
System	4	UDP	imujmu-ae53p0f4	netbios-dgm	*	*		
System	4	UDP	imujmu-ae53p0f4	netbios-ns	*	*		

Figure 8: TCPView of a default Windows 2003 Installation.

As you can see Windows has a variety of services that use TCP. The majority of these do not have a Remote Address. This means that some processes on your computer are communicating, using TCP, with other processes on your computer. This is a standard practice and, for the most part, you will only need to be concerned with suspicious processes connecting to suspicious remote addresses. If you do notice a suspicious TCP connection you can easily right click on the processes and click on End Process. It may be obvious that this tool is very similar to netstat. If you are in a hurry you might save time by using netstat, but TCPView is more powerful and has greater functionality beyond monitoring. You can easily see the process associated with each TCP connection which is very helpful.

5.2 Process Monitor

Process Monitor, called procmon.exe in Sysinternals, is a program that can be used to show what resources each processes is using. Many processes require the usage of different resources that are stored on your computer. Process Monitor will help you understand which resources each process is using. For the most part Process Monitor is an advanced tool to use that takes a lot of technical knowledge to understand what is really being shown, but knowing about this tool is important.

Figure 9 shows a usage for Process Monitor that does not require deep technical knowledge. Using the Process Tree, found in tools, you can easily see how each process was created, and by what processes. This is extremely useful.

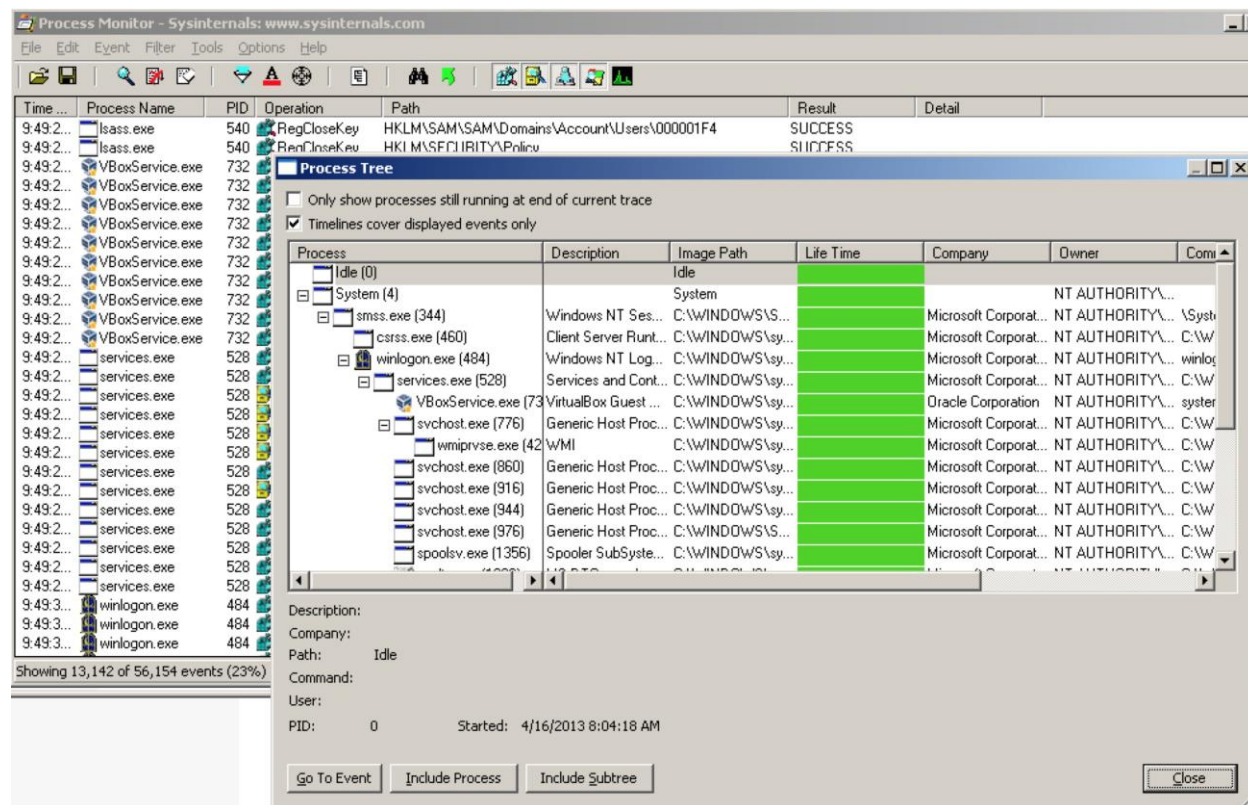


Figure 9: Process Tree example. See how processes were spawned.

Using Process Tree, you can look for suspicious child processes (processes created by others). For example, Firefox.exe should not be spawning Notepad.exe. Processes that have nothing to do with each other should not be spawning each other. If you see this you should investigate the processes using TCPView as you may have been compromised. Spend some time looking at the process tree and noting how one process may spawn many others. Open a program and see how the Process Tree changes.

5.3 Autoruns

One thing an attacker will likely do after hacking a computer is adding in a mechanism to get back into the computer when it is turned off and on. This means the attacker has to set the computer to run a certain program on startup,

otherwise once you turn a computer off all of the attacker's work is gone. To do this they will add a file to an autorun directory or to the Registry. Usually, when applications wish to run at startup, they will be added in msconfig to the autorun tab. Checking this autorun tab is a good start but is not enough. An attacker who knows Windows internals will know there are many places they can put code that they want to be run at start-up. In-fact, there are so many places it would take too long to do this manually. Autoruns is an application that can be used to show ALL programs that will run at start-up. Figure 10 shows how to view all Autorun programs. Open autoruns.exe and select the Everything tab.

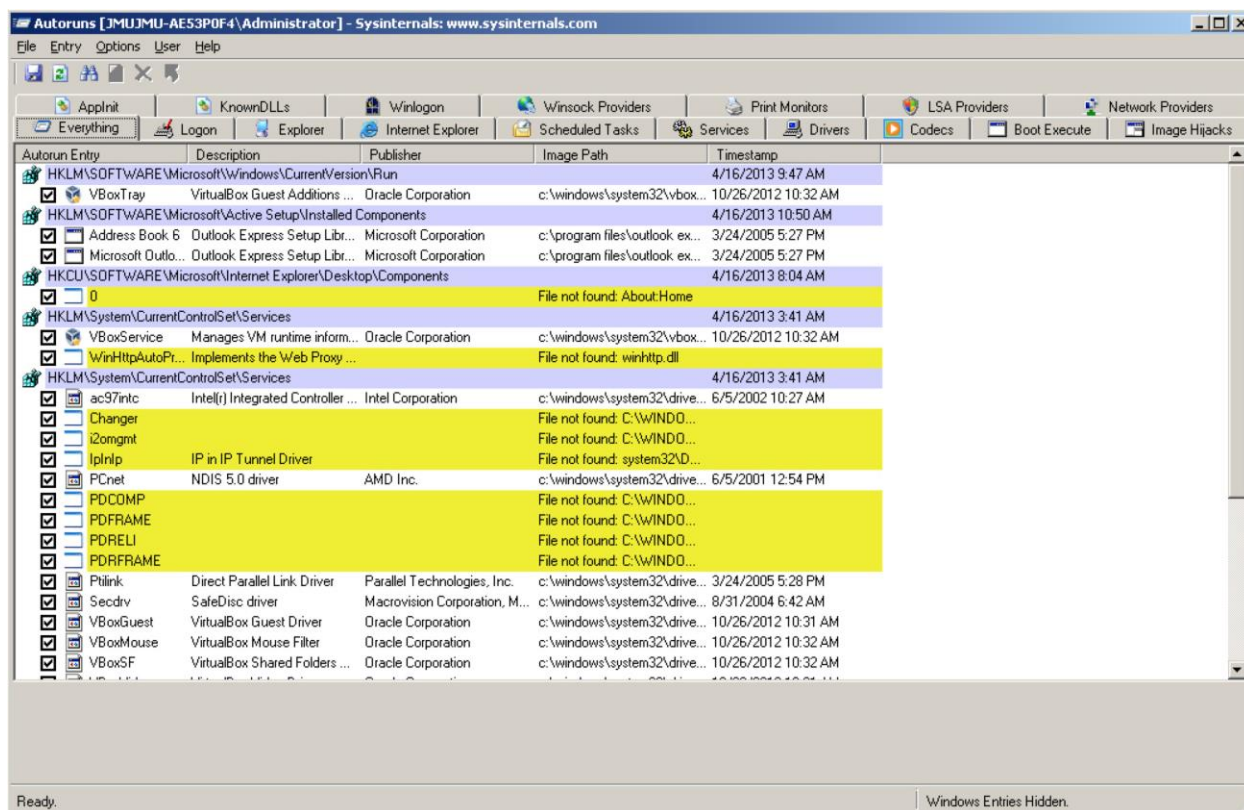


Figure 10: Show all processes that are autorun.

In this Everything tab you should see a lot of things that run at startup that are required for the computer to work properly. They are part of the Windows Operating System. Like the other Sysinternals tools, you should be looking for suspicious programs that auto-run. Suspicious programs would include Services that are being started that you know you should not be required. If an FTP Server is started when you do not need FTP (you should never need FTP), or if a strange

looking .exe is started, you need to investigate this and possibly remove it. Check to see if it is listening for incoming connections with netstat and check TCPView to see if the process has a remote connection to it. Nothing is currently hidden in an autorun directory. There is nothing for you to remove with this tool, but there are many things that run at startup. Take a look around at them. All the functionality that your computer has is accomplished with programs that run at startup. It may be a good idea to familiarize yourself with what a normal set-up looks like, and then look for things that are out of place when the time comes.

5.4 Rootkit Revealer

Sometimes hacker will use sophisticated software to hide their presence on the machine. For example, the software may change the netstat command output to filter out the hacker's connection to your computer. Anyone who uses the netstat command will see regular output from the command, but the hacker's connection will be mysteriously missing. Programs that do this are called Rootkits. They are extremely dangerous and can be difficult to find. In Sysinternals RootkitRevealer.exe can be used to help locate these.

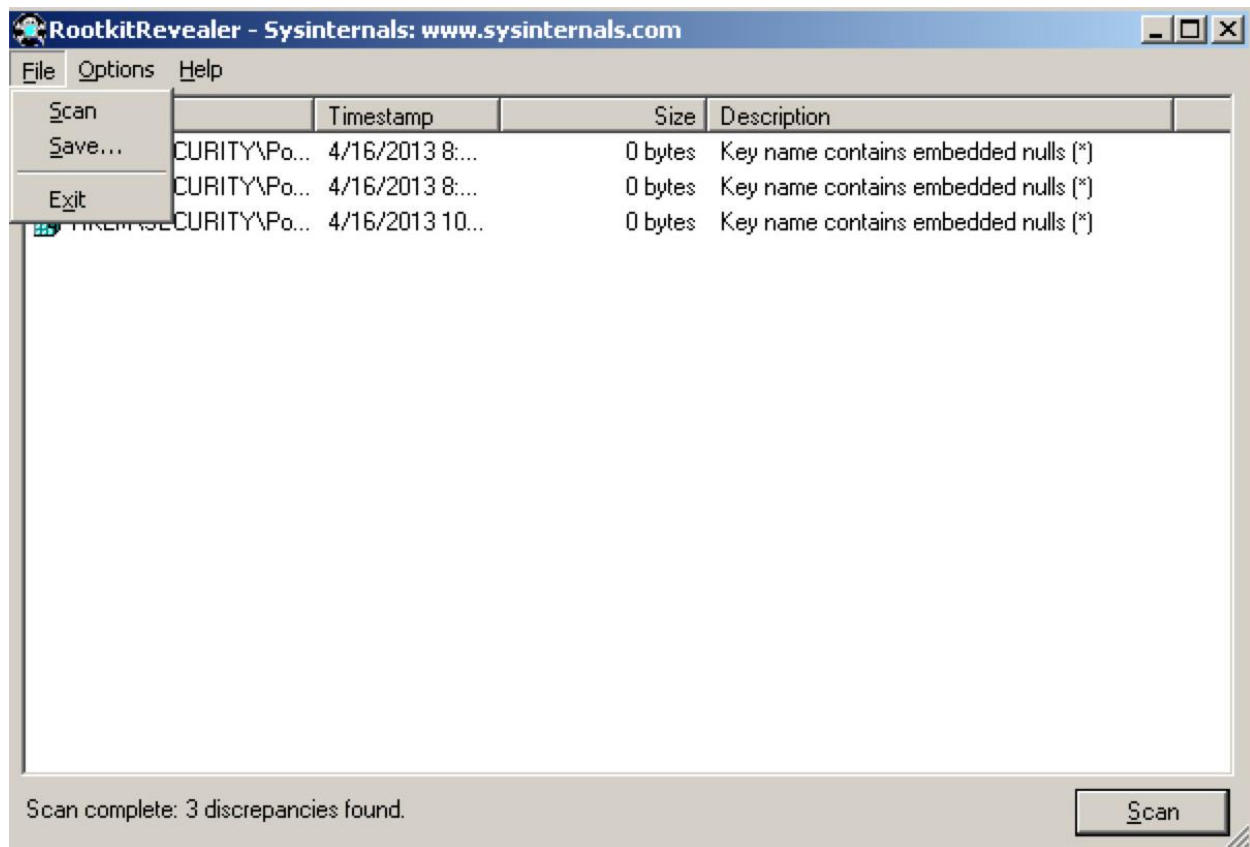


Figure 11: Show all processes that are autorun.

Figure 11 shows how to start a scan and tell your computer to begin looking for rootkits. Rootkit Revealer works by asking for the same information from a lot of different places and trying to find discrepancies. For example, it may ask for open TCP connections. To do this, Rootkit revealer may use netstat, but also ask the underlying operating system. If there is a discrepancy in the information that is returned, Rootkit Revealer will alert you and look for the root cause. Rootkit Revealer, if it finds a well-known rootkit, will also easily allow you to remove it. Rootkits are extremely powerful tools and have gotten extremely advanced and easy to use in the last few years. Rootkit Revealer may help, but as a defender you really do not want to be in a position where you have to remove a rootkit. If Rootkit Revealer doesn't help, you may have a difficult road ahead of you. Remember that, although this is a powerful tool and will do a good job detecting rootkits, it is not foolproof. There is always a chance of a false positive when scanning.

6 EventViewer

The Event viewer is used to view logs as they are generated on your computer. Your computer, by default, logs many things, like successful logins to your computer. What the computer logs can be changed to log more information or to log less information. This is a tradeoff. The more things you log, the more system resources you must dedicate to logging (processing power, writing to disk, and space). Log too little and you are unable to determine what happened if someone hacks your computer. This is an important tradeoff. You can access the Event Viewer in the Computer Management window in Administrative Tools. To change exactly what is logged, you must access the Local Security Policies, in Administrative Tools.

6.1 Change What Is Logged

By default, Windows does not log enough. We would at least like to see failed login attempts instead of only successful. To make windows log these:

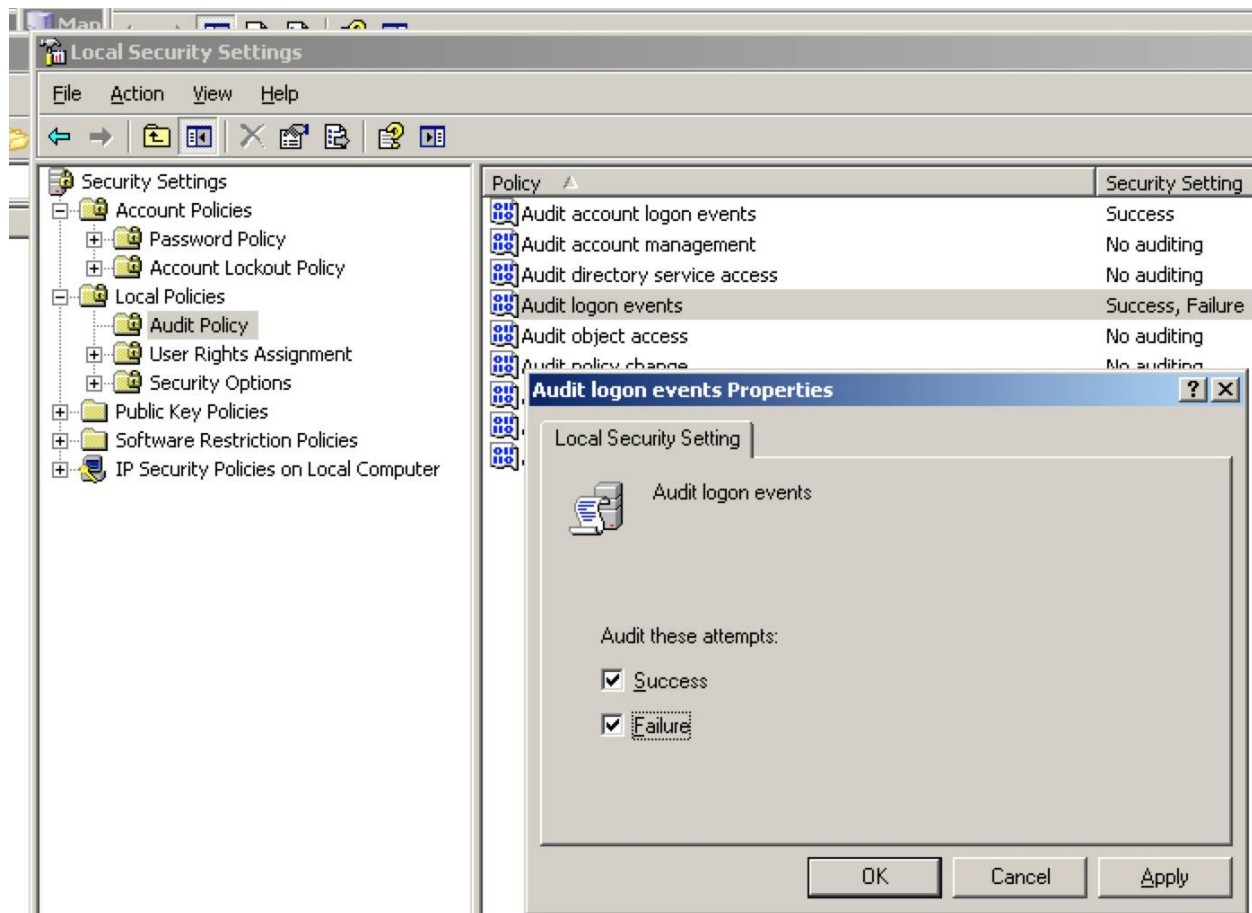


Figure 12: How to add failed login attempts. Remember to press 'apply'

You can view these attempts and see much more information in the event viewer like in Figure 13. Double clicking events in the Event Viewer will provide you with more information. Using the Event Viewer, you may be able to notice if you have been compromised. For example, if you notice many unsuccessful login attempts at one certain time, followed by a successful attempt, it would be a good idea that you should look further into the incident and reset that user's password.

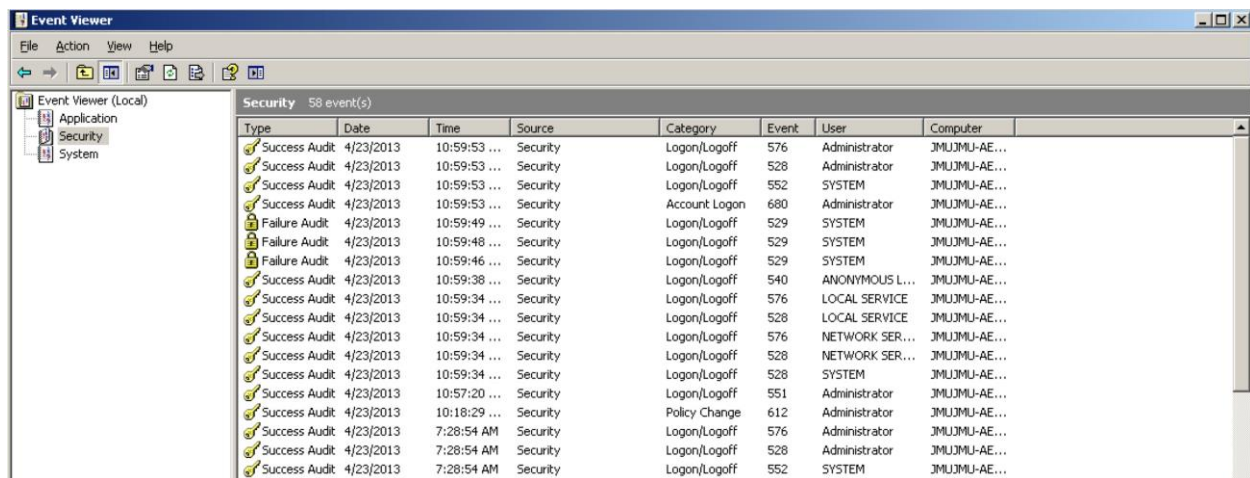


Figure 13: How to add failed login attempts. Remember to press 'apply'

7 Valhalla Honeypots

Honeypots are traps that defenders set on their network in order to attract hackers and allow defenders to easily identify who is malicious on their network. The concept is straightforward. A defender creates a Virtual Machine or a real machine and puts it on their network. The defender makes it look like this machine is very old and vulnerable to attacks (low hanging fruit). Hackers are lazy, so low hanging fruit is very desirable. Since a regular user on the network will never have a need to access the honeypot, any computer that contacts the honeypot is likely compromised. There are different levels of interaction that a honeypot can have. A low interaction honeypot will fool vulnerability scanners but a hacker will never be able to hack or 'log-in'. High interaction Honeypots will fool vulnerability scanners but will also give the attack the illusion that they can log-in or hack the computer. There is a lot of software out there that allows you to easily set up a honeypot on a Windows machine. We will be using software called Valhalla to create honeypots. Valhalla is capable of creating low-interaction and high-interaction honeypots. To use Valhalla, open the Valhalla directory on the desktop and double click the .exe file. Next, click the Server Config button on the left side.

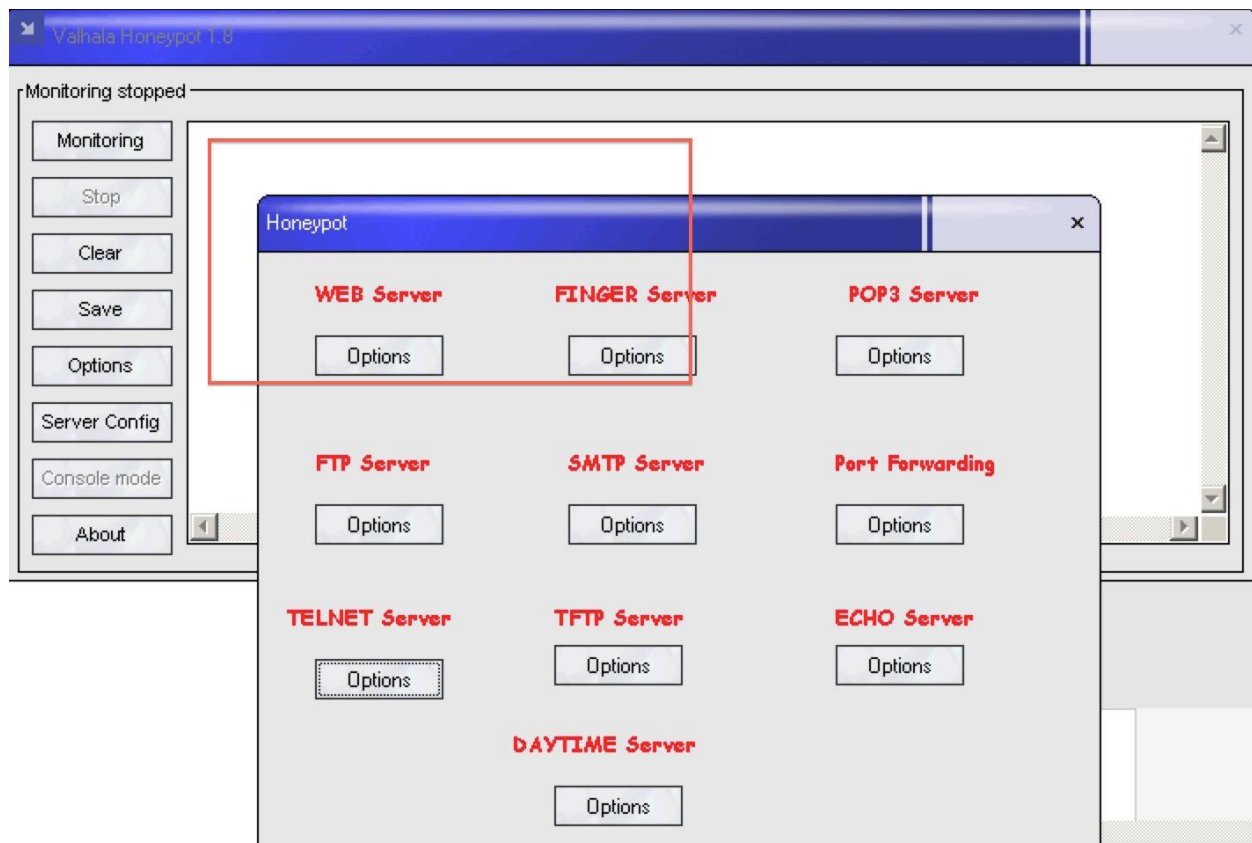


Figure 14: Valhalla Server Config GUI

After opening the Server Config GUI, press the Options button for Web Server, FTP Server, and TELNET Server. Select the Enable buttons you see in Figure 15 and the No Login required button.

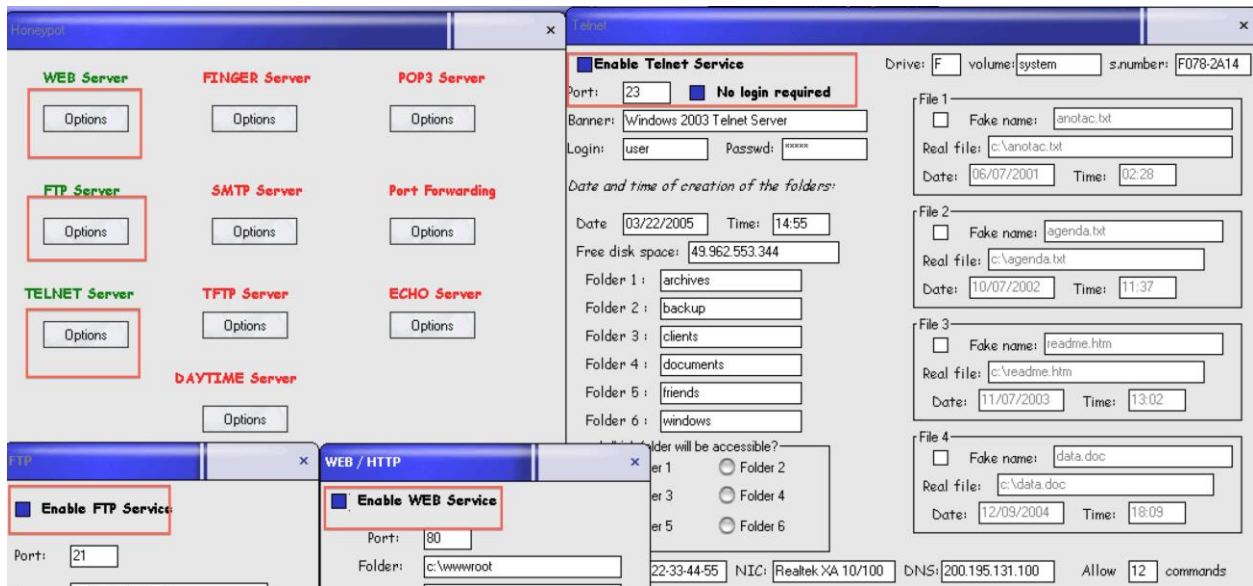


Figure 15: Valhalla Server Config GUI

After clicking the Enable buttons you can X out of the windows and click "Monitoring".

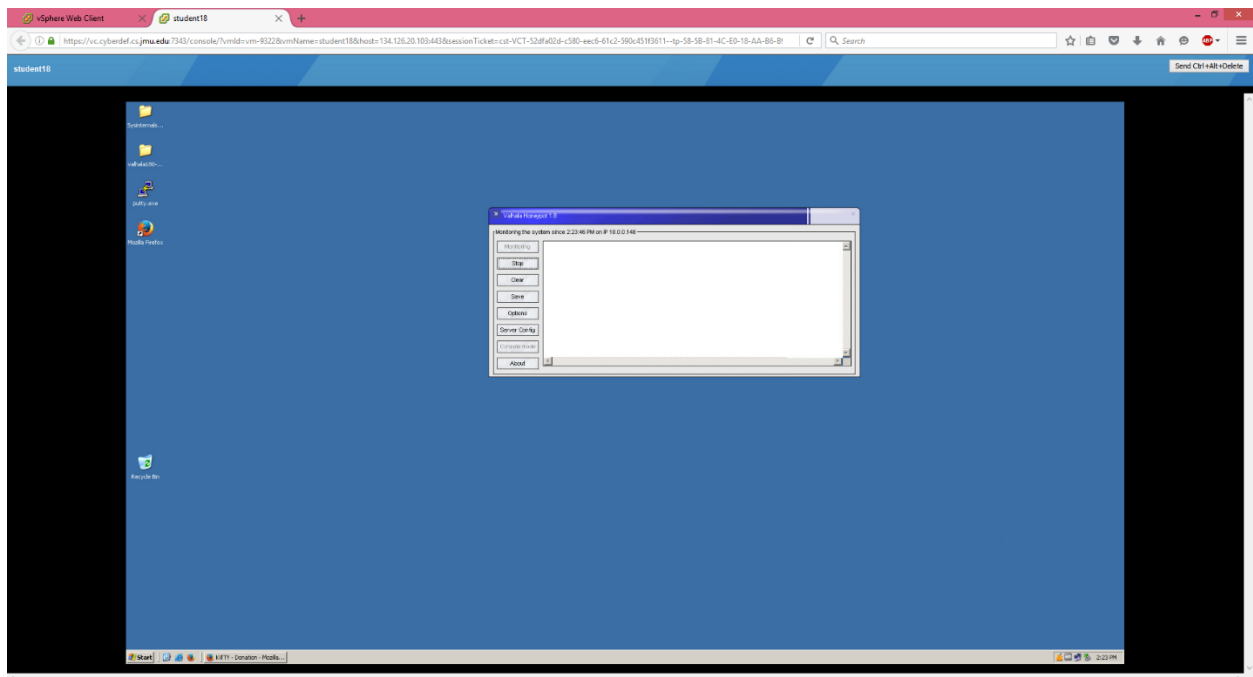


Figure 17: Valhalla monitoring.

Now to test this we can run the TELNET client from the Command Prompt. Within the Command Prompt, type "telnet 127.0.0.1" (as shown in figure 16) and hit ENTER.

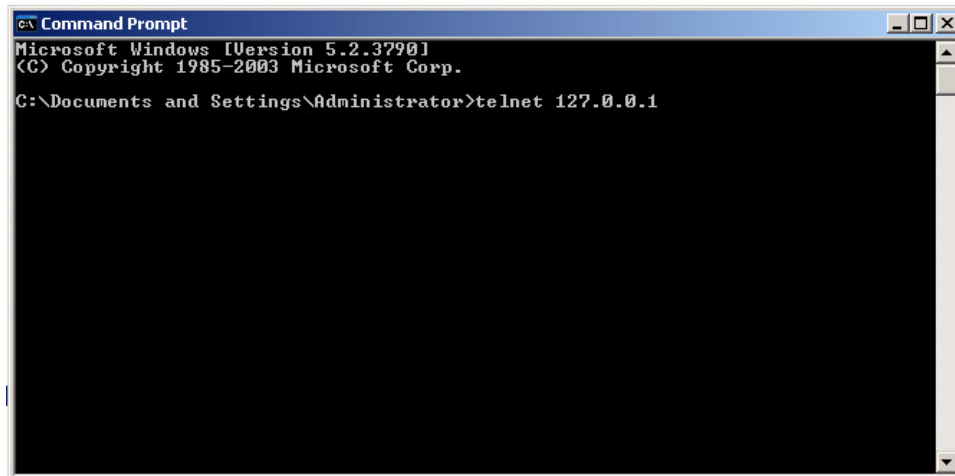


Figure 16: Telnet command within Command Prompt

This will now establish a connection with your Honeypot, which can be seen within the Valhalla monitoring window. If you type commands (none of which should work or do much) they will also be logged by the Honeypot.

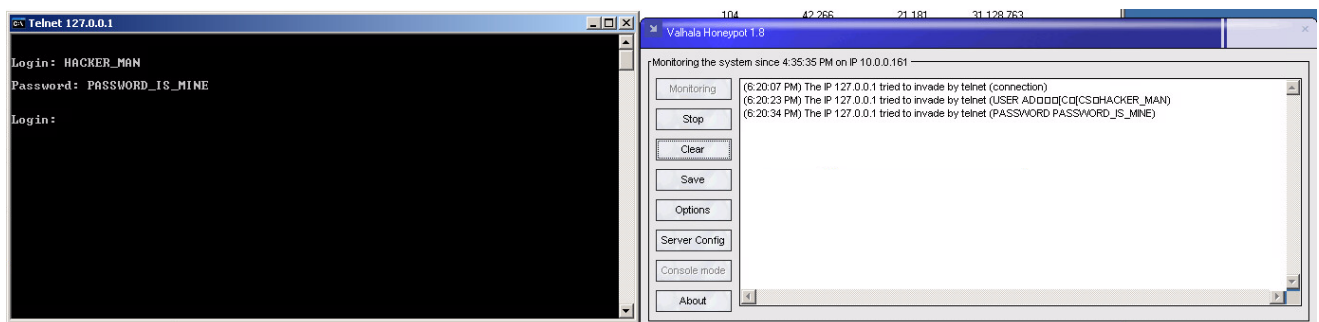


Figure 19: The honeypot at work.

Above was the TELNET part of the Honeypot, but what about WEB? Stopping the monitoring, go back to the WEB client portion of Server Config and go to the Options. Make sure the Folder is "c:\inetpub\wwwroot" and the Index Page is "index.html" as shown in figure 20.

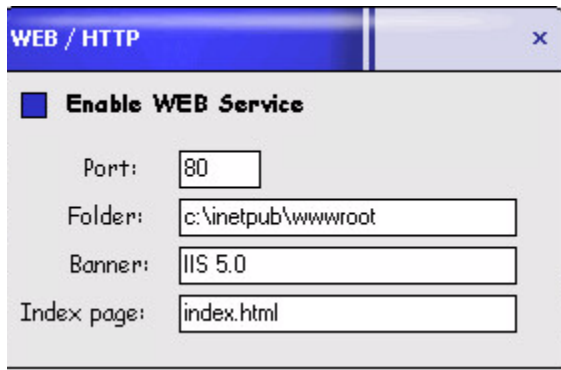


Figure 20: WEB Client Options

Press Start, click Run, and type cmd.exe and hit Enter. This will cause a Command Prompt to open. Next, type echo "Text Webpage" >

C:\inetpub\wwwroot\index.html. This will create a new file, called index.html, that contains "Text Webpage".

After this you can X out of the Valhalla configuration windows and click "Monitoring".

The point of this is that you configured Valhalla to have a Webserver honeypot. This page will be sent to anyone who tries to access your computer on Port 80, because web servers always run on Port 80. To test this, open up a web browser, and in the URL bar type "http://localhost".

8 Conclusion

Responding to an incident can be difficult. Piecing together what happened can be extremely challenging and it is possible that you may never have a complete picture of what happened. This tutorial was showed basic re-hardening and

incident response tools, but there is still much to learn in the future. There was nothing to remove in this exercise because it is a very good idea to see what a non-compromised computer looks like, before you try to decide whether a different computer is compromised. More advanced incident response techniques will all differ depending on what you wish to do following the incident. If you wish to build a case and press charges against the individuals responsible, your course of action will be very different than if you only want your computer to be safe from outsiders.